**Title of the project :** Creating Secured Multi-clouds by Continuous

Automated Auditing using Ternary Hash Tree in AWS

**Name of the students :** Jayalakshmi S, Sai Veena K, Harini A

**Register Numbers :** 211417104089, 211417104122, 211417104503

**Name of the Guide :** Dr. Kavitha Subramani

**ABSTRACT**

There are countless choices for the way to store and access the data. There’s the disc drive on the portable computer, the external disc drive you utilize for backing up and transferring information, network file shares, USB drives, and a lot of. With numerous storage choices accessible, what makes cloud storage more captivating is that files are accessed and altered with ease. Accessing files from any device, anywhere is the key for cloud. Most of the organizations are moving to cloud storage to acquire advantage of the larger information availability, vital value savings, and information redundancy compared to conventional infrastructure. An important element of cloud data security is data integrity — preventing unauthorized modification or deletion and guaranteeing that knowledge remains unchanged since originally uploaded. This can be sometimes monitored by Third-party auditors appointed by the organizations. However, it can lead to high risks associated related to knowledge integrity which incorporates human errors(procrastination), corporate executive threats (the corruption of files), malicious intruders, compromised hardware, and configuration error, etc. This solution aims at resolving the preceding issues. In this work, we tend to plan a unique integrity verification framework in a multi-cloud atmosphere for securing cloud storage with the help of Ternary Hash Tree (THT) and Replica-based Ternary Hash Tree (R-THT). This helps to perform continuous data auditing at fixed time intervals which will be set by the admin. Differing from existing work, the auditing occurs at 3 levels-Block- level, File-level, and Replica-level with tree block ordering, storage block ordering for preserving data-integrity and guaranteeing data availableness within the cloud. The File recovery process will be carried out by the checker automatically if the information gets corrupted while checking. Users will cavil the cloud for file recovery. The outcomes depict that the planned secure cloud auditing framework is very secure and economical in storage, communication, and computation prices.